FIG. 1A

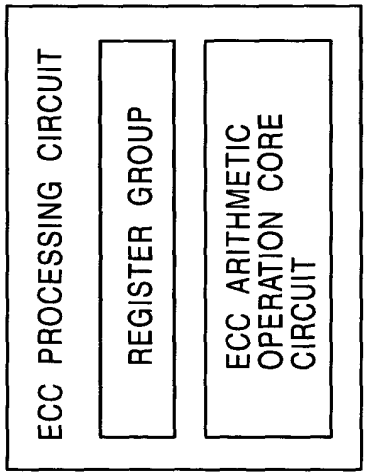



FIG. 1B

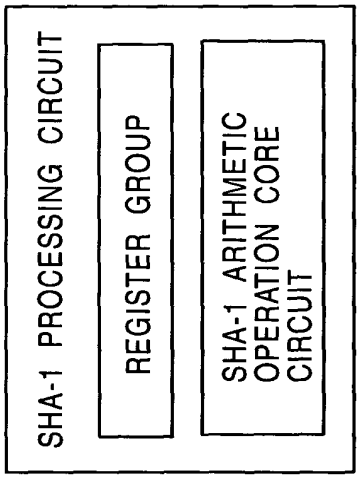



FIG. 1C

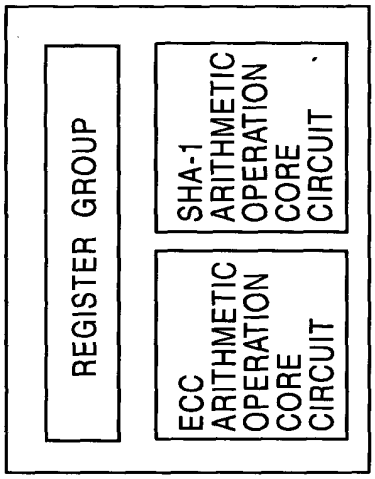


FIG. 2

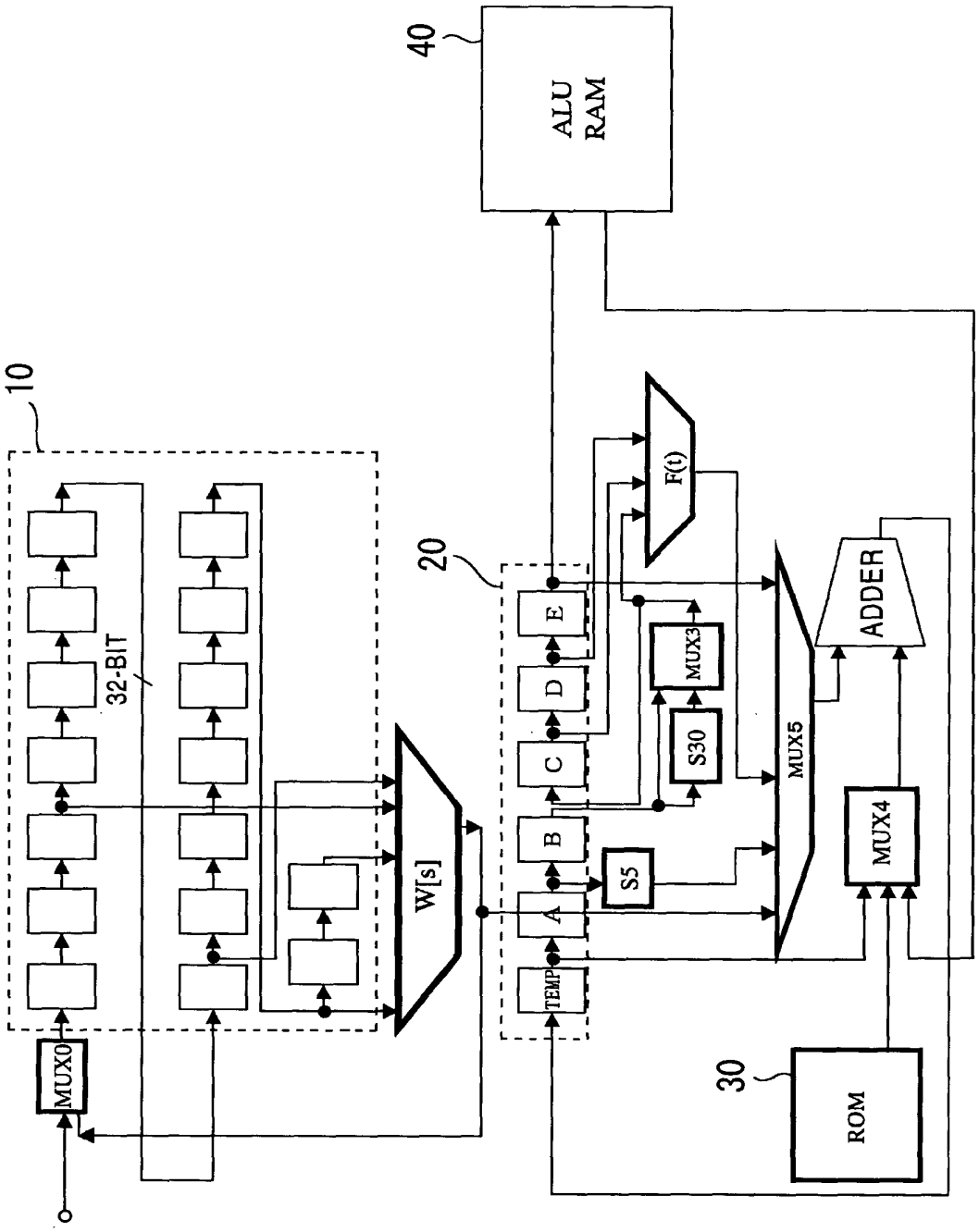

40
ALU
RAM
10
32-BIT
MUX0
W[s]
20
F(t)
E
D
C
B
A
TEMP
MUX3
S30
S5
MUX5
ADDER
MUX4
30
ROM

FIG. 3

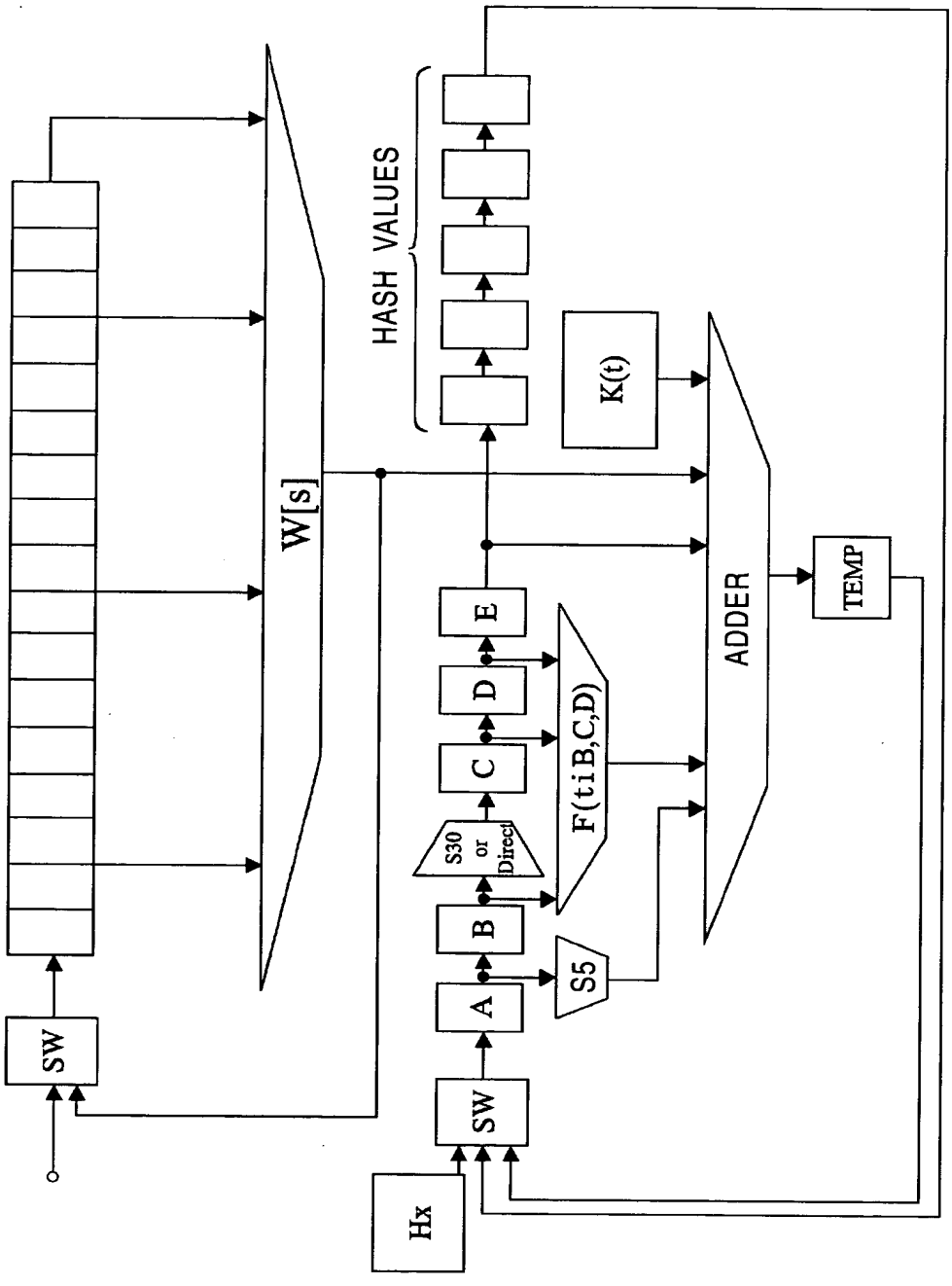

SW
W[s]
HASH VALUES
K(t)
ADDER
TEMP
E
D
C
S30 or Direct
F(tiB,C,D)
B
S5
A
SW
Hx

FIG. 4

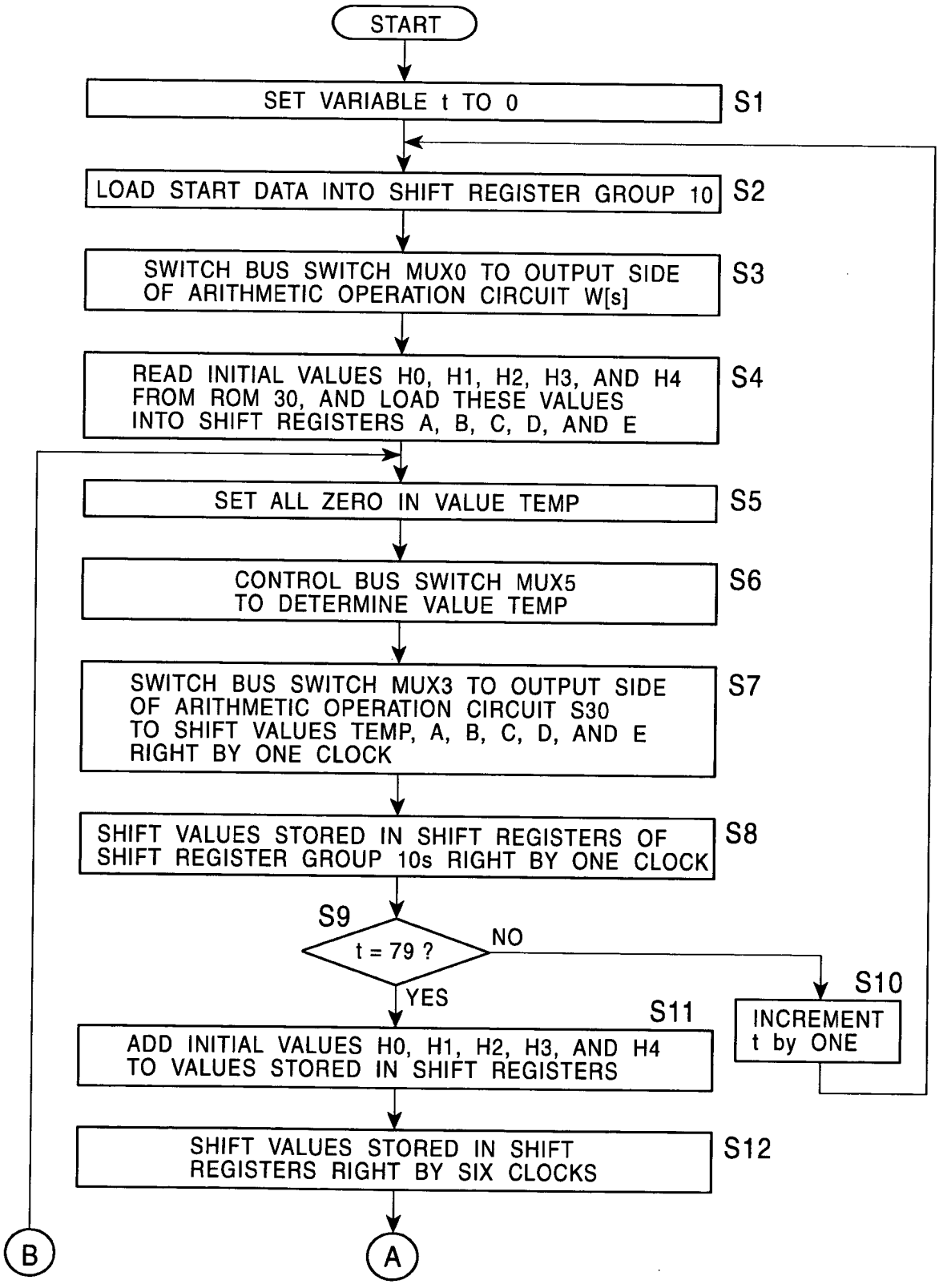

START
SET VARIABLE t TO 0
S1
LOAD START DATA INTO SHIFT REGISTER GROUP 10
S2
SWITCH BUS SWITCH MUX0 TO OUTPUT SIDE OF ARITHMETIC OPERATION CIRCUIT W[s]
S3
READ INITIAL VALUES H0, H1, H2, H3, AND H4 FROM ROM 30, AND LOAD THESE VALUES INTO SHIFT REGISTERS A, B, C, D, AND E
S4
SET ALL ZERO IN VALUE TEMP
S5
CONTROL BUS SWITCH MUX5 TO DETERMINE VALUE TEMP
S6
SWITCH BUS SWITCH MUX3 TO OUTPUT SIDE OF ARITHMETIC OPERATION CIRCUIT S30 TO SHIFT VALUES TEMP, A, B, C, D, AND E RIGHT BY ONE CLOCK
S7
SHIFT VALUES STORED IN SHIFT REGISTERS OF SHIFT REGISTER GROUP 10s RIGHT BY ONE CLOCK
S8
S9
t = 79 ?
NO
YES
S10
INCREMENT t by ONE
S11
ADD INITIAL VALUES H0, H1, H2, H3, AND H4 TO VALUES STORED IN SHIFT REGISTERS
SHIFT VALUES STORED IN SHIFT REGISTERS RIGHT BY SIX CLOCKS
S12
B
A

FIG. 5

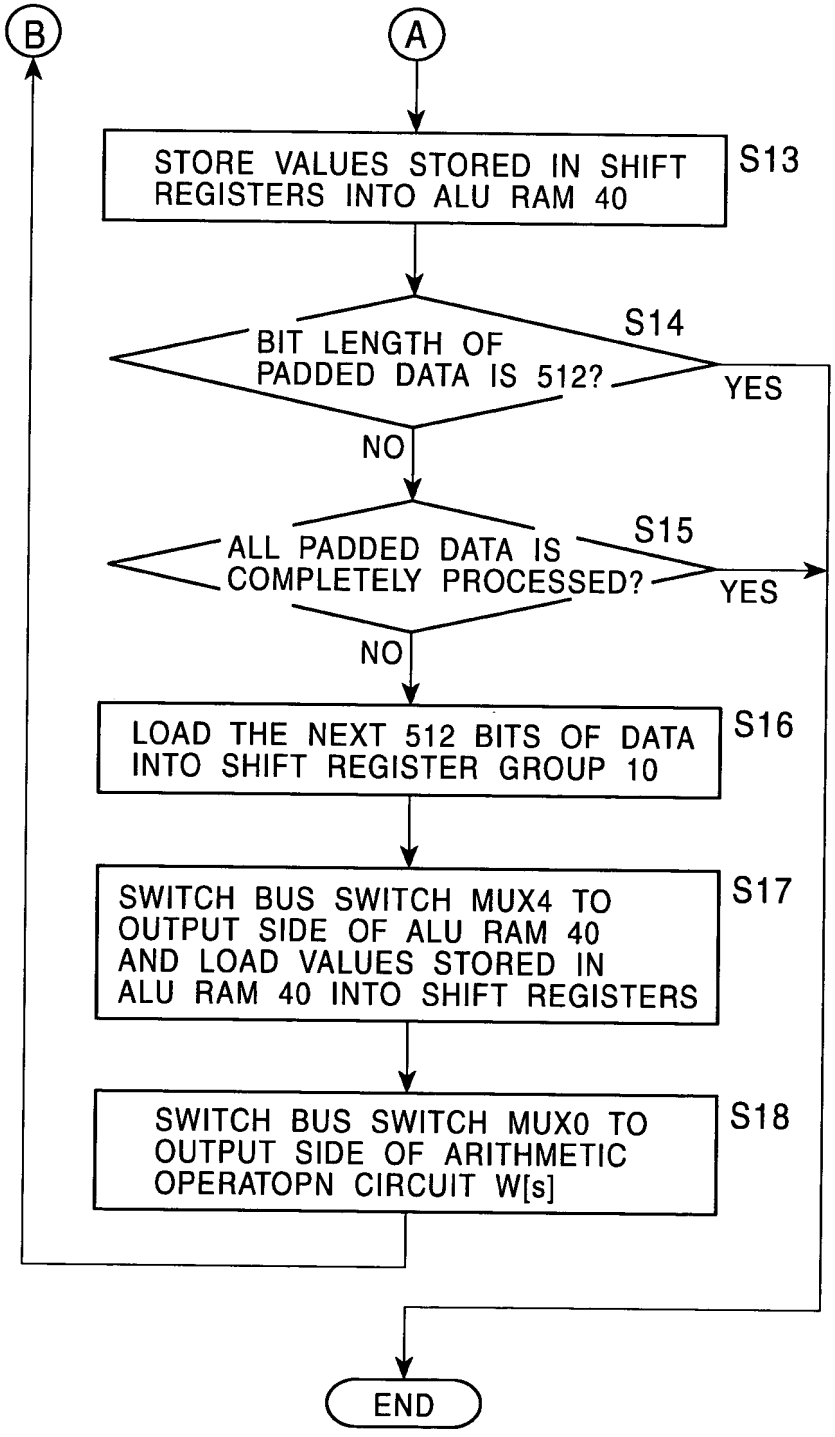
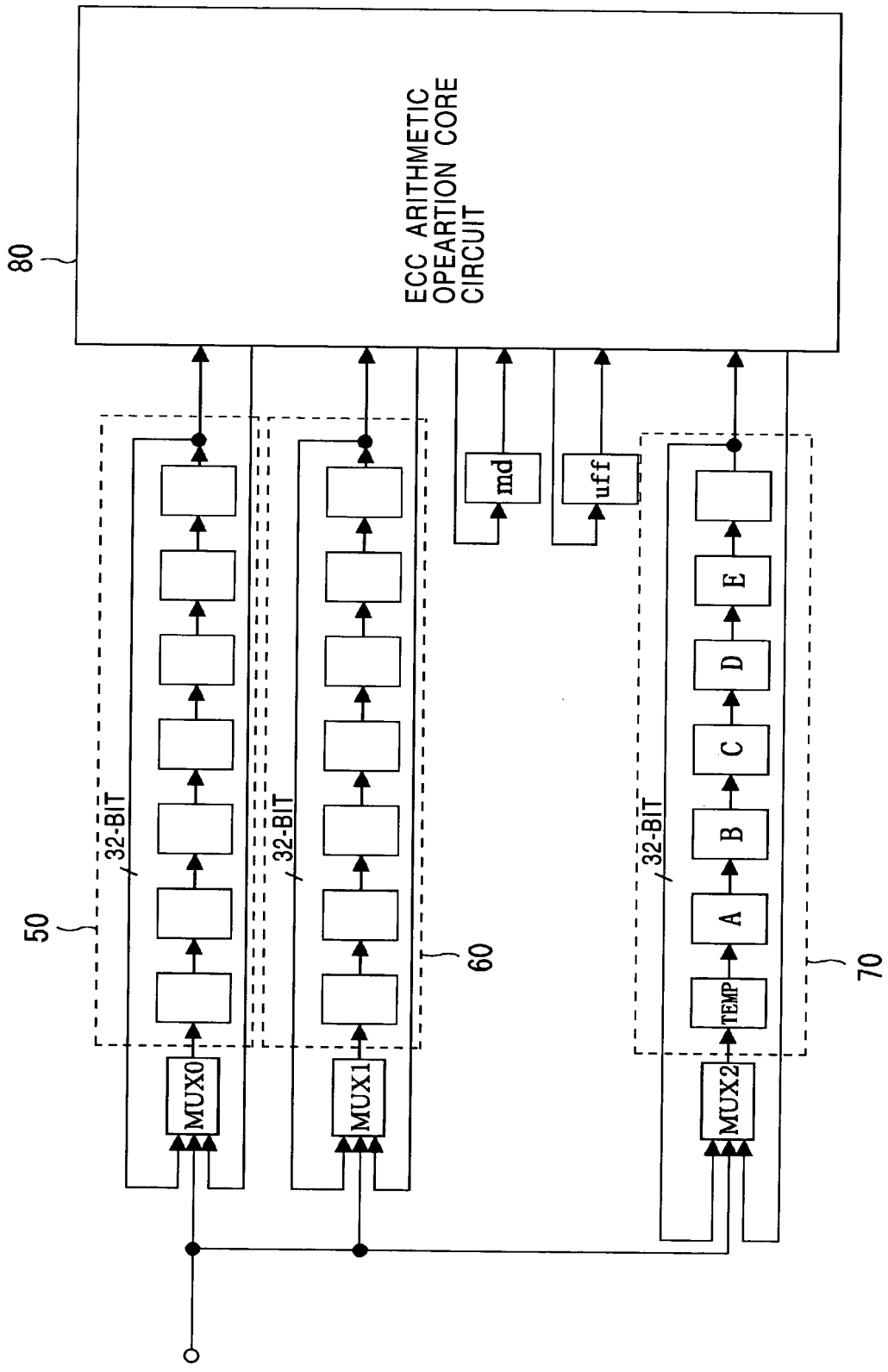

B
A
STORE VALUES STORED IN SHIFT REGISTERS INTO ALU RAM 40
S13
BIT LENGTH OF PADDED DATA IS 512?
S14
YES
NO
ALL PADDED DATA IS COMPLETELY PROCESSED?
S15
YES
NO
LOAD THE NEXT 512 BITS OF DATA INTO SHIFT REGISTER GROUP 10
S16
SWITCH BUS SWITCH MUX4 TO OUTPUT SIDE OF ALU RAM 40 AND LOAD VALUES STORED IN ALU RAM 40 INTO SHIFT REGISTERS
S17
SWITCH BUS SWITCH MUX0 TO OUTPUT SIDE OF ARITHMETIC OPERATOPN CIRCUIT W[s]
S18
END

FIG. 6


80
ECC ARITHMETIC OPEARTION CORE CIRCUIT
md
uff
50
32-BIT
MUX0
60
32-BIT
MUX1
70
32-BIT
TEMP
A
B
C
D
E
MUX2

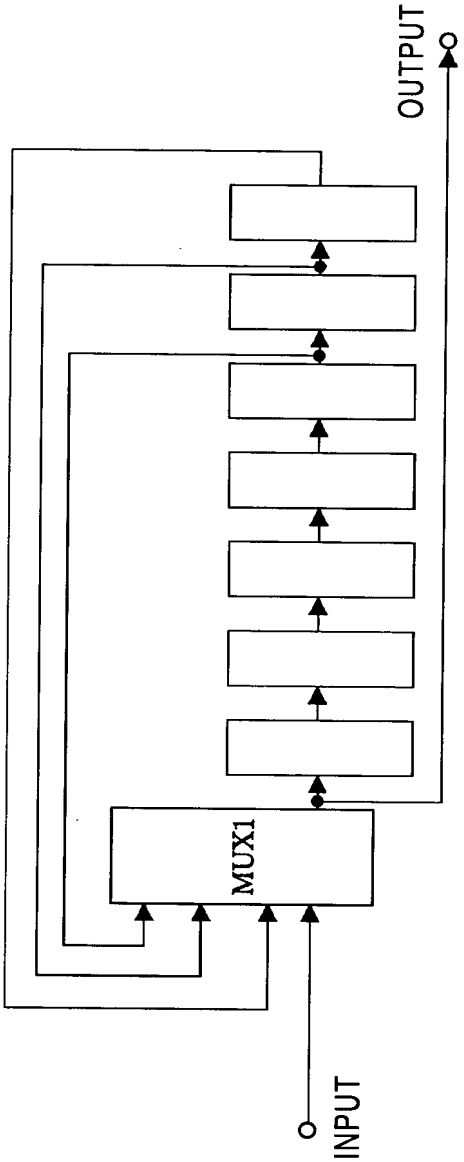



FIG. 7A

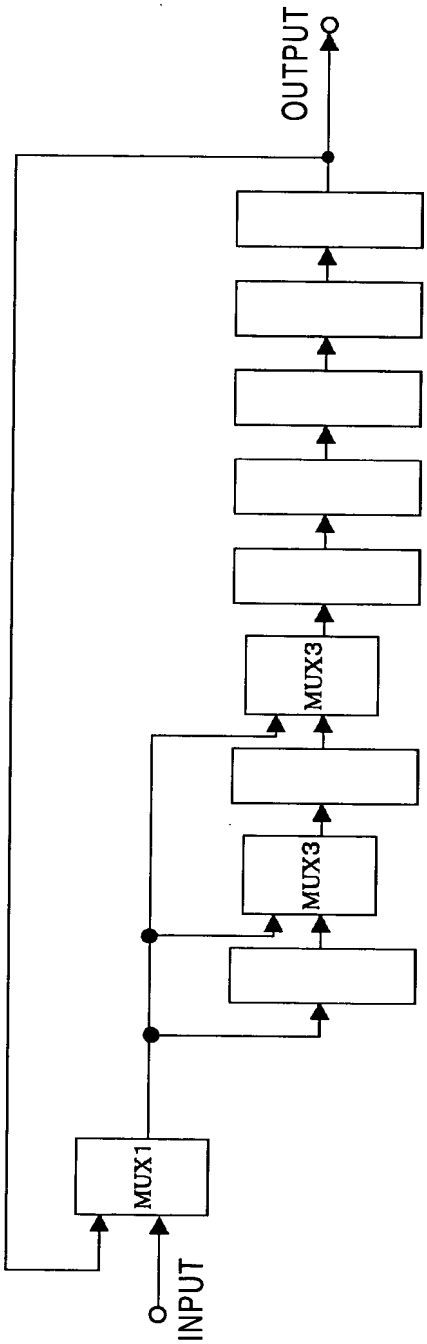
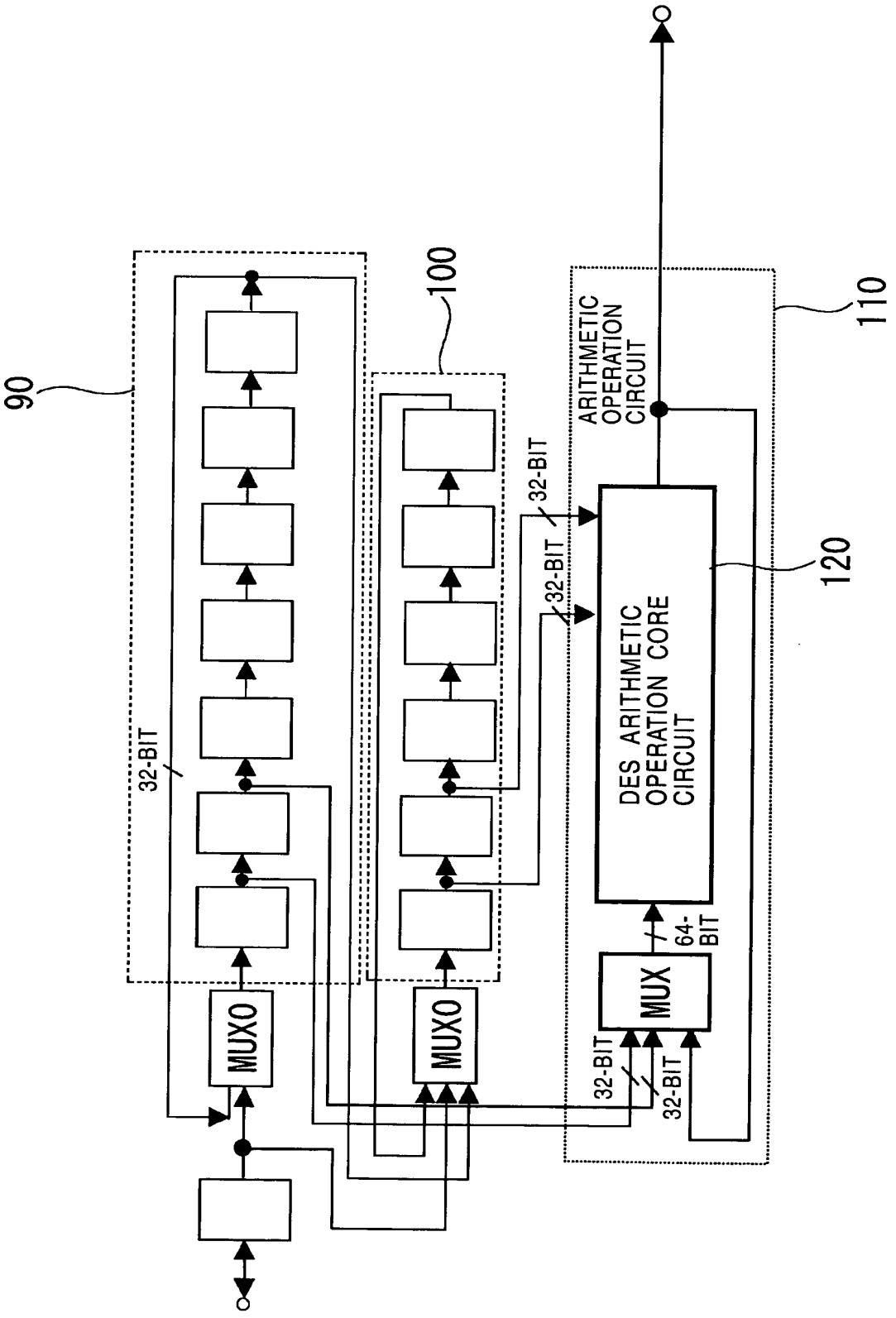



FIG. 7B

FIG. 8


90
100
110
120
32-BIT
32-BIT
32-BIT
ARITHMETIC OPERATION CIRCUIT
DES ARITHMETIC OPERATION CORE CIRCUIT
MUX0
MUX0
MUX
64-BIT
32-BIT
32-BIT

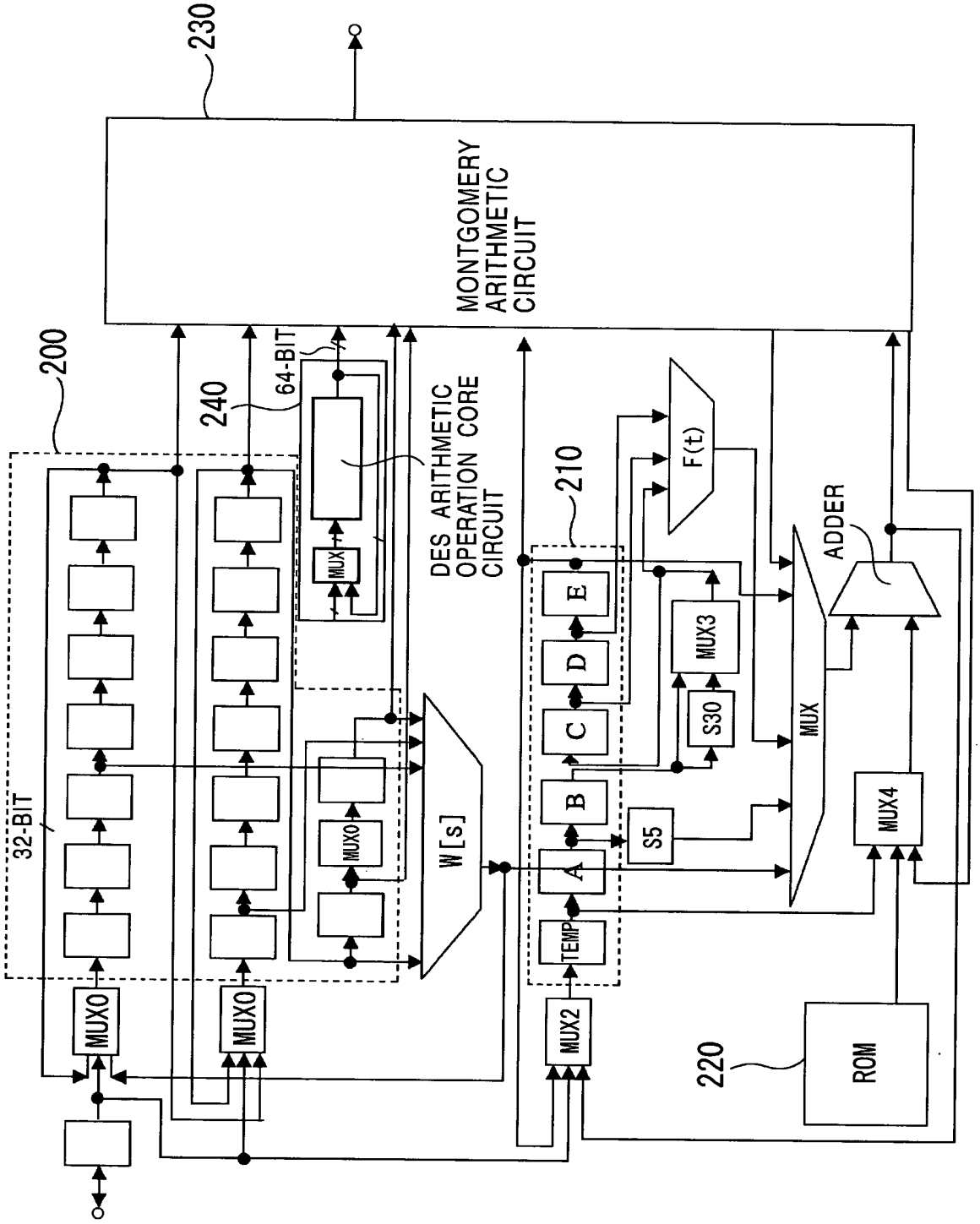

230
MONTGOMERY ARITHMETIC CIRCUIT
200
240
64-BIT
DES ARITHMETIC OPERATION CORE CIRCUIT
210
F(t)
ADDER
MUX
MUX3
S30
E
D
C
B
A
TEMP
S5
MUX4
MUX2
MUX0
MUX0
MUX0
MUX
W[s]
32-BIT
220
ROM

FIG. 9

FIG. 10

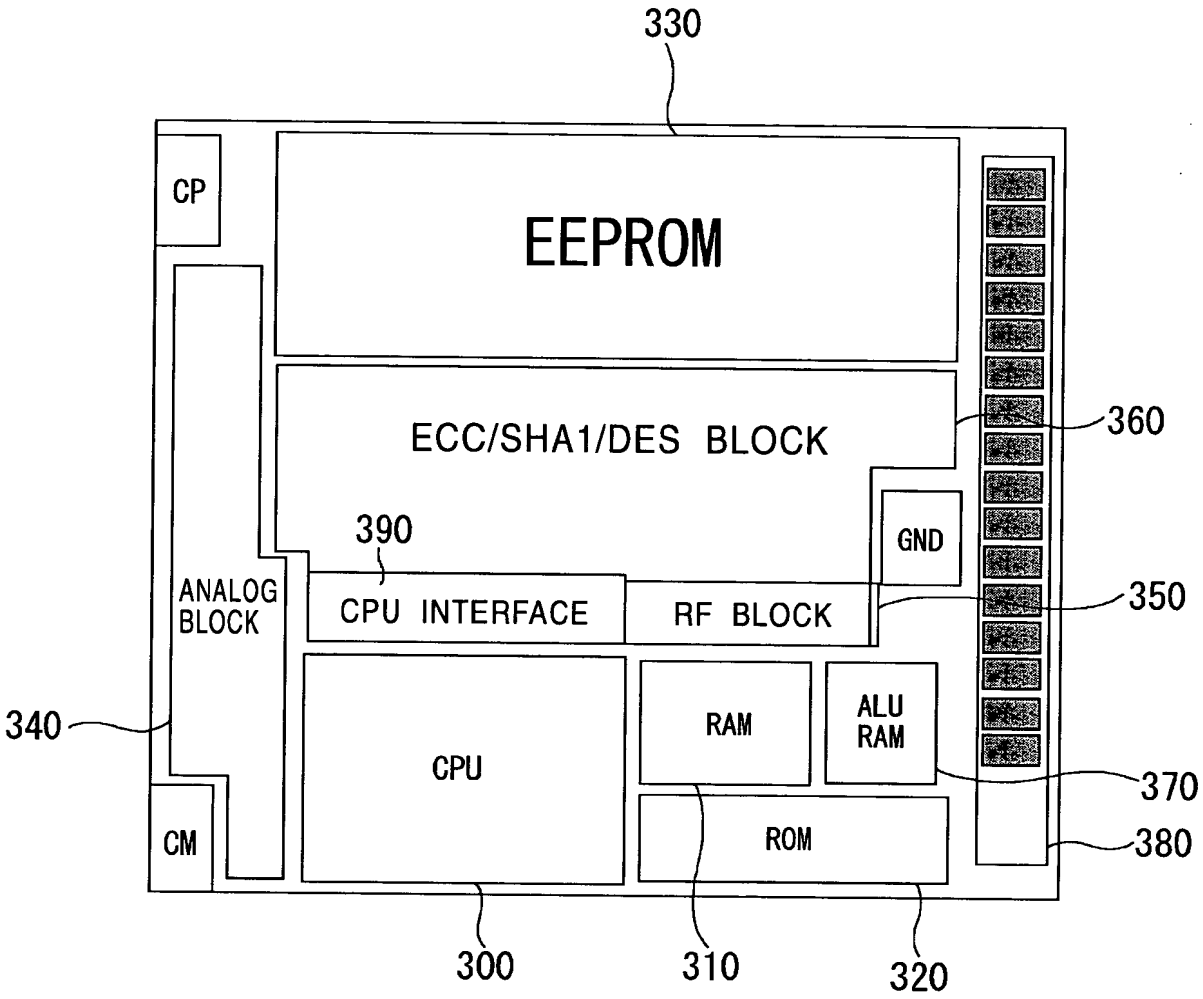

330
CP
EEPROM
ECC/SHA1/DES BLOCK
360
390
GND
ANALOG BLOCK
CPU INTERFACE
RF BLOCK
350
340
CPU
RAM
ALU RAM
370
CM
ROM
380
300
310
320

FIG. 11

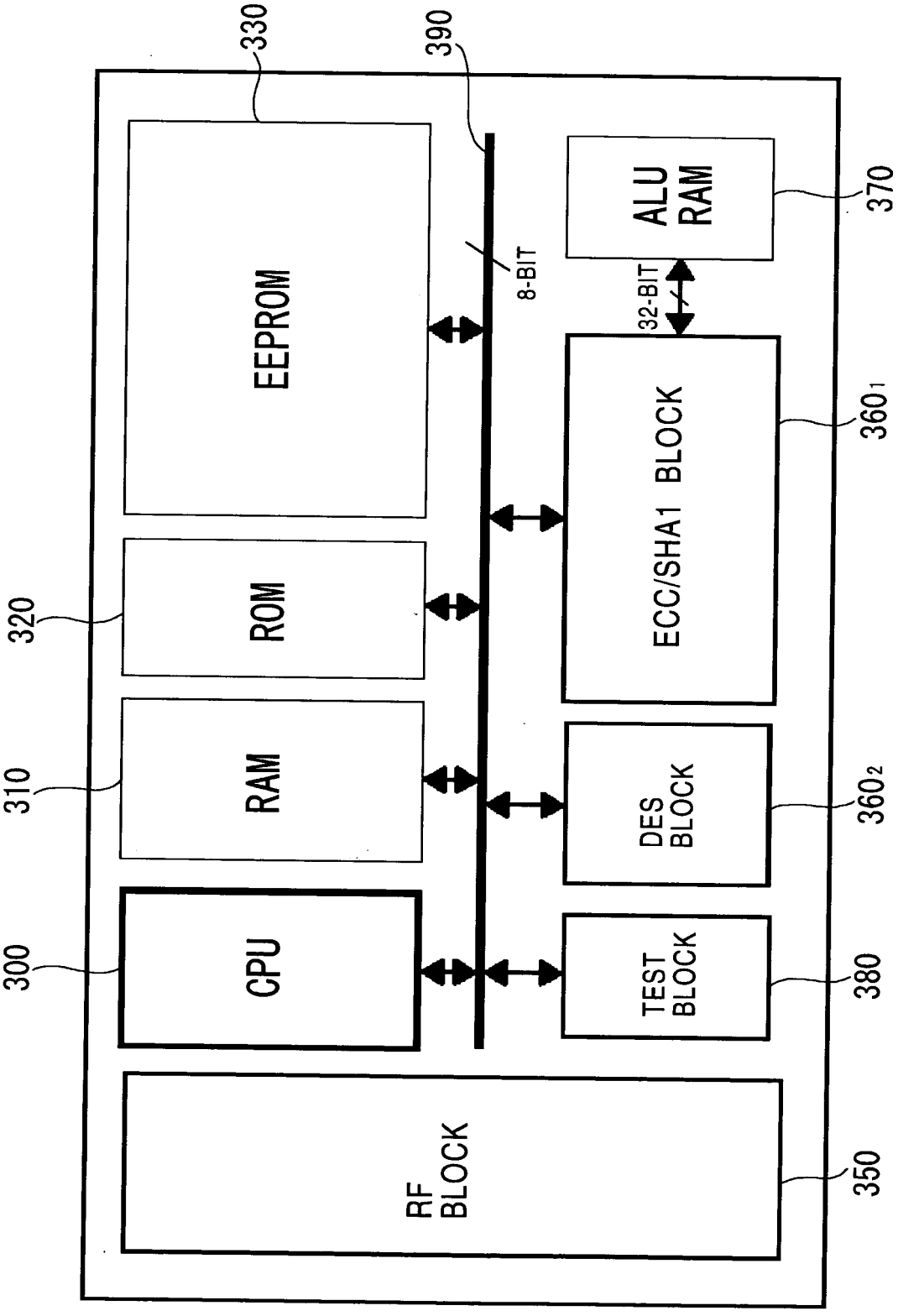

330
390
EEPROM
8-BIT
ALU RAM
370
32-BIT
ECC/SHA1 BLOCK
360₁
320
ROM
310
RAM
DES BLOCK
360₂
300
CPU
TEST BLOCK
380
RF BLOCK
350

FIG. 12A

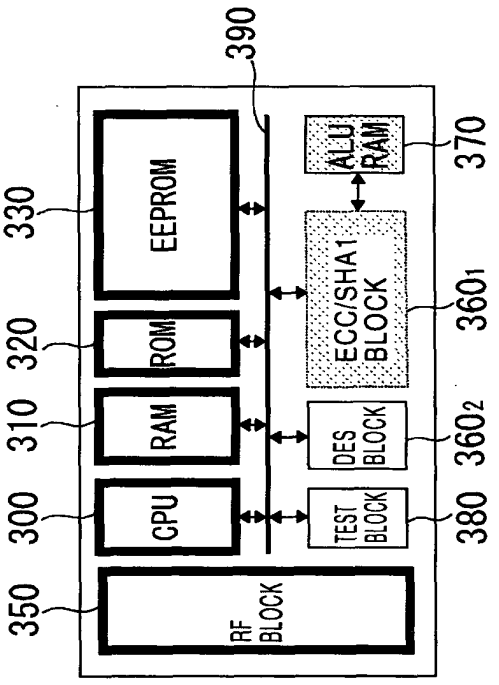



FIG. 12B

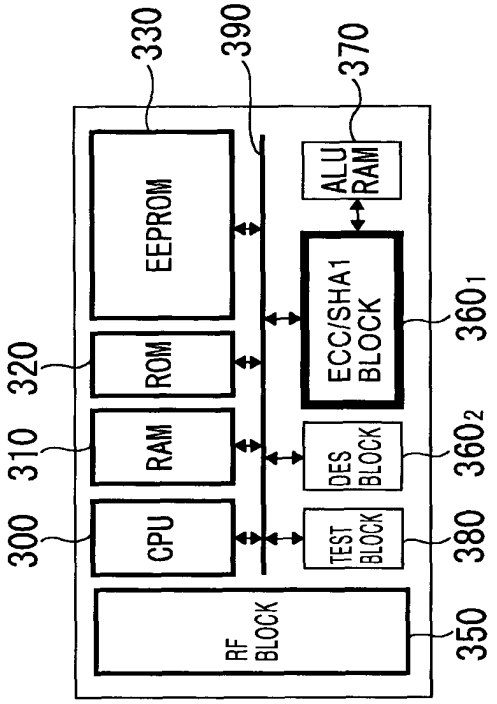



FIG. 12C

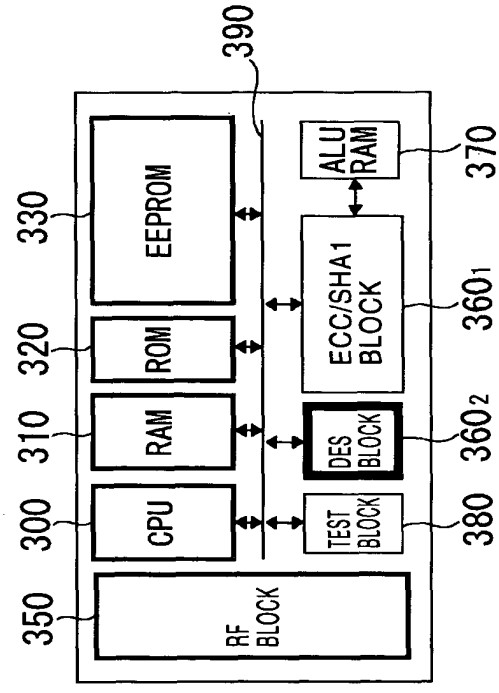



FIG. 12D

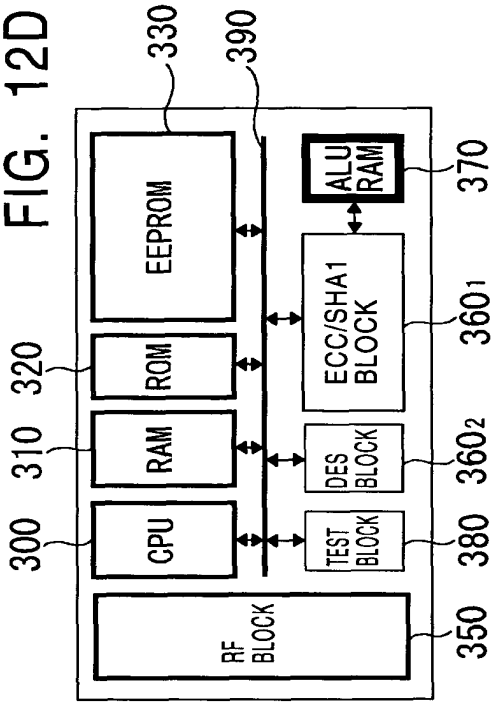


FIG. 13A

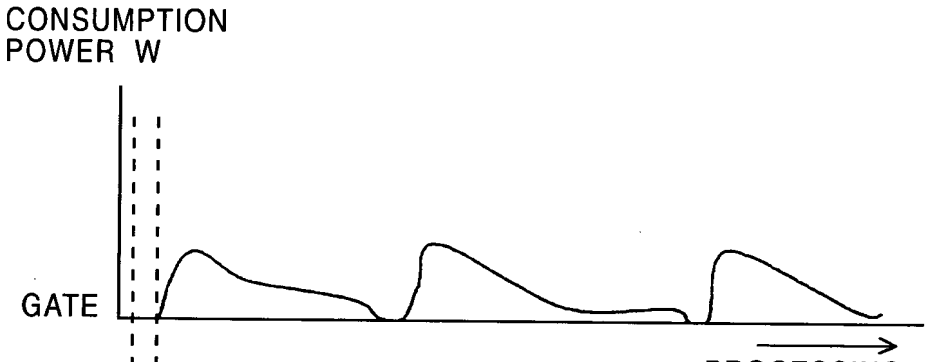



FIG. 13B


FIG. 13C

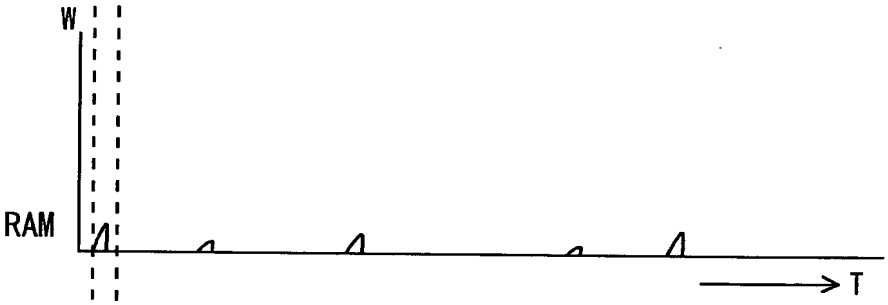



FIG. 13D

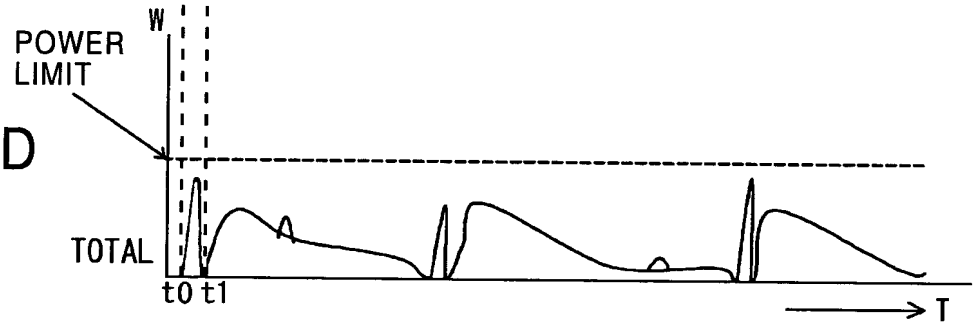


FIG. 14A

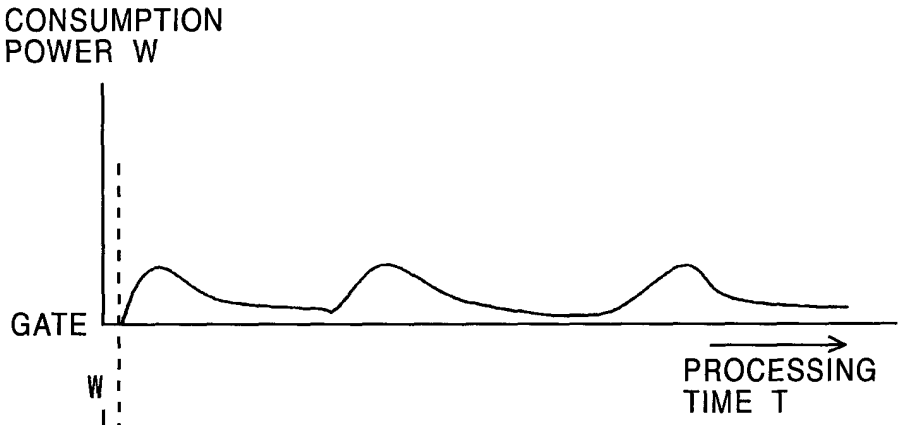



FIG. 14B

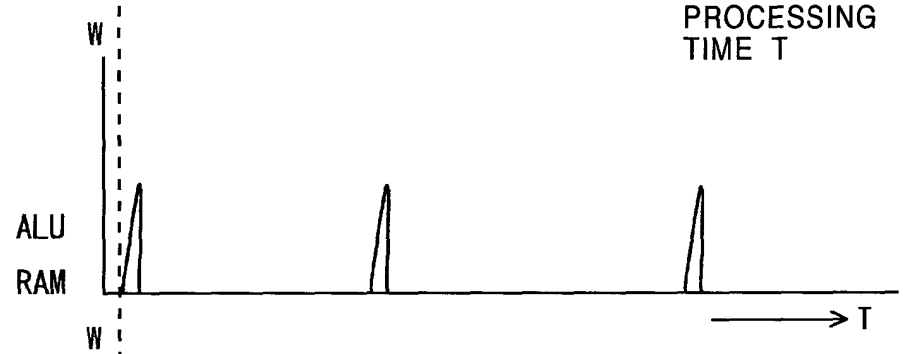



FIG. 14C

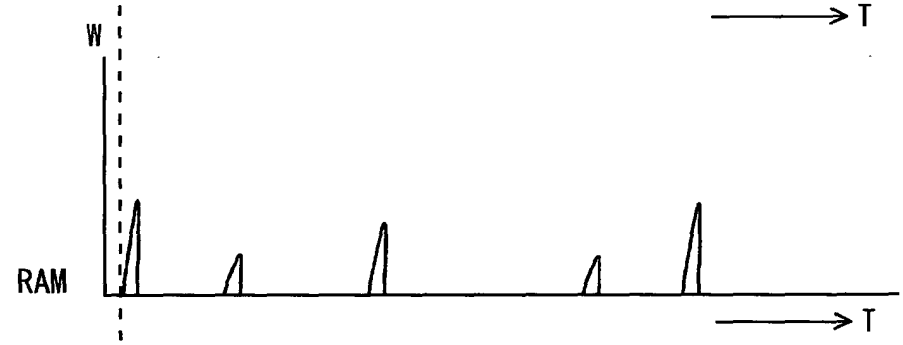



FIG. 14D